

**MEMORANDUM OF LAW IN SUPPORT OF MOTION TO COMPEL
COMPLIANCE WITH THIRD-PARTY SUBPOENAS**

TABLE OF CONTENTS

TABLE OF AUTHORITIES	ii
I. PARTIES TO THIS MOTION	1
A. Plaintiffs	1
B. Defendants.....	2
II. PROCEDURAL HISTORY.....	3
A. The <i>Hake</i> Action	3
B. The <i>Gill</i> Action.....	4
III. RELEVANT BACKGROUND OF UNDERLYING <i>HAKE</i> ACTION	5
A. The <i>Hake</i> Defendants	5
1. Bank Markazi	6
2. Bank Melli	6
3. National Iranian Oil Company	7
B. Iran Requires Access to U.S. Dollars and U.S. Dollar-Clearing Mechanisms	7
C. Defendants Processed U.S. Dollar-Denominated Transactions on Behalf of Iran and Its Agents and Instrumentalities	9
1. SCB.....	9
2. SocGen.....	10
3. BNPP	11
4. HSBC.....	12
5. NatWest	14
IV. THE SUBPOENA REQUESTS	14
A. The <i>Hake</i> Subpoena	14
B. The <i>Gill</i> Subpoenas	15
V. THE SUBPOENA RECIPIENTS' NON-COMPLIANCE.....	16
A. Six Subpoena Recipients Have Made Insufficient Productions.....	16
B. Two Subpoena Recipients Have Not Produced at All	20
1. HSBC.....	20
2. NatWest	21
VI. LEGAL ARGUMENT.....	22
A. The Information Sought by Plaintiffs Is Relevant to Their Claims.....	23
VII. CONCLUSION.....	25

TABLE OF AUTHORITIES

Cases

<i>Asad Gilani v. Hewlett Packard Co.</i> , No. 15-CV-05609 (NSR), 2017 WL 4236564 (S.D.N.Y. Sept. 22, 2017)	22
<i>Banco Cent. De Paraguay v. Paraguay Humanitarian Found., Inc.</i> , No. 01 CIV. 9649 (JFK), 2006 WL 3456521 (S.D.N.Y. Nov. 30, 2006)	23
<i>Citizens Union of City of New York v. Atty. Gen. of N.Y.</i> , 269 F. Supp. 3d 124 (S.D.N.Y. 2017)	22
<i>Condit v. Dunne</i> , 225 F.R.D. 100 (S.D.N.Y. 2004)	22
<i>EM Ltd. v. Republic of Argentina</i> , 695 F.3d 201 (2d Cir. 2012)	24
<i>Estate of Heiser v. Bank of Tokyo Mitsubishi UFJ, New York Branch</i> , 919 F. Supp. 2d 411 (S.D.N.Y. 2013)	6
<i>Fireman’s Fund Ins. Co. v. Great Am. Ins. Co. of N.Y.</i> , 284 F.R.D. 132 (S.D.N.Y. 2012)	23
<i>Flanagan v. Islamic Republic of Iran</i> , 87 F. Supp. 3d 93 (D.D.C. 2015)	24
<i>In re Terrorist Attacks on Sept. 11, 2001</i> , No. 03 MDL 1570 (GBD), 2011 WL 13244047 (S.D.N.Y. Dec. 22, 2011)	5, 7
<i>Licci ex rel. Licci v. Lebanese Canadian Bank, SAL</i> , 732 F.3d 161 (2d Cir. 2013)	8
<i>Maresco v. Evans Chemetics, Div. of W.R. Grace & Co.</i> , 964 F.2d 106 (2d Cir. 1992)	22
<i>Oppenheimer Fund, Inc. v. Sanders</i> , 437 U.S. 340 (1978)	22
<i>Republic of Argentina v. NML Capital, Ltd.</i> , 573 U.S. 134 (2014)	23

Statutes

22 U.S.C. § 8513a	6
28 U.S.C. § 1605A	1, 3, 4

28 U.S.C. § 1608.....	4
Iran Threat Reduction and Syria Human Rights Act of 2012, Pub. L. 112-158, 126 Stat. 1214 (Aug. 10, 2012).....	7
Terrorism Risk Insurance Act, Pub. L. 107-297, 116 Stat 2322 (Nov. 26, 2002).....	24
Other Authorities	
Executive Order 13382, 70 Fed. Reg. 38567 (June 28, 2005).....	7
Permanent Subcomm. on Investigations of the Comm. on Homeland Security and Governmental Affairs, 112th Cong., S. Hrg. 112-597 (July 17, 2012).....	19
Rules	
Fed. R. Civ. P. 26.....	1, 22, 24
Fed. R. Civ. P. 30.....	25
Fed. R. Civ. P. 34.....	1
Fed. R. Civ. P. 45.....	1, 14
Fed. R. Civ. P. 69.....	1, 22, 23

Pursuant to Federal Rules of Civil Procedure 26, 34, 45, and 69, Plaintiff-movants (“Plaintiffs”) move to compel 8 third-party banks (the “subpoena recipients” or “defendants”) to comply with several subpoenas. As discussed further below, Plaintiffs issued the subpoenas in two separate civil suits brought against Iran and its agents and instrumentalities (“Iranian defendants”) pursuant to the Terrorism Exception to the Foreign Sovereign Immunities Act (“FSIA”), 28 U.S.C. § 1605A. The subpoenas request transactional messages from 2003-2010 (the “relevant period”) relating to U.S. dollar-denominated transactions performed or initiated by or for the Iranian defendants and other related entities. Despite months (in some cases, a year and a half) of attempting to work with the subpoena recipients in good faith, two have not produced a single transaction; the other six have only produced spreadsheets providing inadequate summary data as to an insufficient number of transactions. Plaintiffs respectfully request that the Court compel all eight subpoena recipients to fully comply with the subpoenas.

I. PARTIES TO THIS MOTION

A. Plaintiffs

Plaintiffs are Kelli D. Hake, on behalf of the plaintiffs in *Kelli D. Hake, et al., v. Bank Markazi Jomhouri Islami Iran, et al.*, No. 17-cv-114 (TJK) (D.D.C.) (the “*Hake* plaintiffs” and the “*Hake* action”) and Mati Gill, plaintiff in *Mati Gill v. Islamic Republic of Iran*, No. 15-cv-2272 (RBW) (D.D.C.) (the “*Gill* action”). All of these plaintiffs were injured in terrorist attacks committed by the Islamic Republic of Iran (“Iran”) through its agents, including its paramilitary force, the Islamic Revolutionary Guard Corps (“IRGC”), the IRGC’s “Qods Force” foreign operations directorate (“IRGC-QF”), and its Lebanese terror proxy, Hezbollah.

The *Hake* plaintiffs seek documents to help them meet their burden of proof to establish that defendants Bank Markazi Jomhouri Islami Iran (the Central Bank of Iran, hereafter “Bank Markazi” or “CBI”), Bank Melli Iran (“Bank Melli”) and the National Iranian Oil Company

(“NIOC”) – all Iranian agents and instrumentalities – provided material support to the IRGC, IRGC-QF, Hezbollah, and other Iranian agents and proxies responsible for orchestrating the terror attacks on the *Hake* plaintiffs. In mid-2018, the *Hake* plaintiffs served 31 subpoenas on several banks, including each of the defendants to this motion, seeking transactions relating to the *Hake* defendants and their agents.

Mati Gill already prevailed in his action against Iran (Mr. Gill did not sue any Iranian agencies or instrumentalities), and seeks Iranian assets to satisfy the judgment he was awarded. In September of 2017, Mati Gill served two sets of subpoenas on eight banks, including five defendants to this motion, seeking transactions that may locate or identify assets belonging to Iran or its agents, particularly entities related to the IRGC and Hezbollah.

B. Defendants

Bank of America, N.A. (“BOA”) is a financial services company headquartered in Charlotte, North Carolina. Its New York City office is subject to oversight and regulation by the Board of Governors of the U.S. Federal Reserve System (the “Federal Reserve”) and the New York State Department of Financial Services (“NYSDFS”).

Citibank N.A. (“Citibank”) is a financial services company headquartered in New York City. Citibank’s New York branch is subject to oversight and regulation by the Federal Reserve System and the NYSDFS.

JPMorgan Chase Bank, N.A. (“JPMC”) is a financial services company headquartered in New York City. It is subject to oversight and regulation by the Federal Reserve and the NYSDFS.

HSBC Bank USA, N.A. (“HSBC”) is a financial services company incorporated in Maryland with its operational head office in New York City, where it is supervised and regulated by the Federal Reserve and the NYSDFS. It is a subsidiary of HSBC, which is headquartered in the United Kingdom.

NatWest is a financial services company that is part of The Royal Bank of Scotland Group (“RBS”), which is headquartered in the United Kingdom. NatWest’s New York operations are supervised and regulated by the Federal Reserve and the NYSDFS.

BNP Paribas S.A. (“BNPP”) is a financial services company headquartered in Paris, France. It is the largest bank in France and one of the five largest banks in the world in terms of assets. Its U.S. headquarters is located in New York City. BNPP’s New York branch is subject to oversight and regulation by the Federal Reserve and the NYSDFS.

Société Générale S.A. (“SocGen” or “SG”) is a financial services company headquartered in Paris, France. Its U.S. headquarters is in New York City. SocGen’s New York branch is subject to oversight and regulation by the Federal Reserve and the NYSDFS.

Standard Chartered Bank (“SCB”) is a financial services company headquartered in the United Kingdom. SCB’s New York branch and operations are supervised and regulated by the Federal Reserve and the NYSDFS.

II. PROCEDURAL HISTORY

A. The *Hake* Action

On January 17, 2017, the *Hake* plaintiffs filed a civil action for wrongful death, personal injury and related torts pursuant to the FSIA’s Terrorism Exception. Plaintiffs are American service members who, while serving in a peacekeeping capacity in Iraq, were injured or killed in terrorist attacks occurring from 2004-2011, as well as members of their families. The *Hake* plaintiffs alleged that the *Hake* defendants provided material support to Hezbollah, the IRGC, and other Iranian proxies on Iran’s behalf for these attacks. *See* 28 U.S.C. § 1605A. Much of this material support came in the form of U.S. dollar-denominated transactions that were “cleared” through New York by correspondent banks, including defendants here. The *Hake* plaintiffs’ operative complaint (the Second Amended Complaint) is annexed hereto as Exhibit A.

On July 11, 2017, the Clerk of the D.C. District Court entered defaults for Bank Markazi, Bank Melli, and NIOC. However, even in cases of default, the FSIA requires a claimant “to establish[] his claim or right to relief by evidence satisfactory to the court.” 28 U.S.C. § 1608(e). As a result, on May 2, 2018, the *Hake* court “ORDERED that Plaintiffs may issue third-party subpoenas and Touhy requests in light of Defendants’ default.”

Between May 11 and July 2, 2018, the *Hake* plaintiffs served subpoenas upon financial institutions, including the defendants here, which likely conducted extensive U.S. dollar clearing activities during the relevant time period for Iranian entities, including the *Hake* defendants. Some of the subpoena recipients admitted in Deferred Prosecution Agreements (“DPAs”) or consent orders with U.S. federal or state regulators to engaging in illegal transactions performed on behalf of Iranian entities, others were once listed by NIOC as preferred banks, and still others were among the largest American banks that performed a significant proportion of the dollar-clearing activities in the United States.

Given what appeared to be productive discussions with the subpoena recipients, the *Hake* court extended Plaintiffs’ deadline for filing motions to compel third-party discovery from October 15, 2018 to January 15, 2019 (at which time Plaintiffs moved to compel production from four banks in the related motion to compel, *Hake, et al. v. Credit Suisse, et al.*, Docket No. 19-mc-24 (VEC) (S.D.N.Y.)), and again to March 15, 2019 for certain subpoena recipients (there is no corresponding deadline for third-party post-judgment discovery in the *Gill* action). Despite Plaintiffs’ best efforts, they must now move against the eight bank defendants here.

B. The *Gill* Action

On December 31, 2015, Mati Gill, sued Iran pursuant to 28 U.S.C. § 1605A, for injuries he received during a 2008 Hamas-perpetrated terrorist attack. The court found Iran liable for

providing material support to Hamas, and awarded Mr. Gill \$30 million. *See Exhibit B.* Mr. Gill subsequently commenced post-judgment discovery with respect to Iranian assets with the ultimate goal of recovering on his judgment. Between September and November 2017, Mr. Gill served a total of 15 subpoenas on eight banks, five of which—JPMC, BOA, HSBC, Citibank and SCB—are at issue here. HSBC had not produced a single transaction thus far; the other banks have made insufficient productions. Therefore, Mr. Gill joins this motion to compel the production of documents specified in his subpoenas.

III. RELEVANT BACKGROUND OF UNDERLYING *HAKE* ACTION

During the U.S. occupation of Iraq and its subsequent peacekeeping mission, Iran orchestrated a terror campaign against U.S. service members, civilian personnel and Iraqi civilians. Iran financed this campaign largely through its extensive U.S.-dollar denominated accounts held outside the U.S. (such accounts are called “Eurodollar” accounts). Eurodollar transfers are generally “cleared” through the U.S., meaning Iran required access to the U.S. financial system to access these accounts. *Hake* defendants processed billions of dollars of U.S. dollar-denominated transactions on Iran’s behalf through the United States; where U.S. sanctions prohibited the conduct, the *Hake* defendants worked with certain Western financial institutions to evade those sanctions. Through this process, the *Hake* defendants directed hundreds of millions of U.S. dollars to Hezbollah, the IRGC and the IRGC-QF, which used those resources to carry out the terrorist attacks at issue in *Hake* (and in *Gill*).

A. The *Hake* Defendants

Each of the *Hake* defendants are Iranian state-controlled entities used in the service of financing terrorism. *See, e.g., In re Terrorist Attacks on Sept. 11, 2001*, No. 03 MDL 1570 (GBD), 2011 WL 13244047, at *6 (S.D.N.Y. Dec. 22, 2011) (“The entire apparatus of the Iranian state and government, and many parts of Iran’s private sector, including corporations (*e.g.*, National

Iranian Oil Company, Iran Air, Iran Shipping Lines); banks (*e.g.*, Central Bank, Bank *Sepah*); . . . private individuals; and even charities are at the service of the Supreme Leader [and] the IRGC . . . when it comes to support of terrorism.”).

1. Bank Markazi

Bank Markazi, Iran’s central bank, has provided millions of dollars to terrorist organizations via other Iranian-owned and controlled banks. According to the U.S. Treasury and Congress: “The Central Bank of Iran, which regulates Iranian banks, has assisted designated Iranian banks by transferring billions of dollars to these banks in 2011. In mid-2011, the CBI transferred several billion dollars to designated banks, including Saderat, Mellat, EDBI and Melli, through a variety of payment schemes.” 22 U.S.C. § 8513a (designating the “financial sector of Iran as of primary money laundering concern.”). Moreover, “Bank Saderat . . . has been used by the Government of Iran to channel funds to terrorist organizations, including Hezbollah and . . . Hamas;” for instance, “from 2001 to 2006, Bank Saderat transferred \$50 million from the Central Bank of Iran through its subsidiary in London to its branch in Beirut for the benefit of Hezbollah fronts in Lebanon that support acts of violence.”¹

2. Bank Melli

Bank Melli, one of the largest banks in Iran, was nationalized following the Iranian Revolution in 1979. *See Estate of Heiser v. Bank of Tokyo Mitsubishi UFJ, N.Y. Branch*, 919 F. Supp. 2d 411, 418-19 (S.D.N.Y. 2013) (“[T]he Central Bank of Iran expressly recognizes Bank Melli Iran as a ‘commercial government-owned bank.’”). According to the U.S. government:

Bank Melli also provides banking services to the [IRGC] and the Qods Force. Entities owned or controlled by the IRGC or the Qods Force use Bank Melli for a

¹ Press Release, U.S. Dep’t of the Treasury, “Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism” (Oct. 25, 2007), available at <https://www.treasury.gov/press-center/press-releases/pages/hp644.aspx>.

variety of financial services. From 2002 to 2006, Bank Melli was used to send at least \$100 million to the Qods Force. When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement from the international banking system. For example, Bank Melli has requested that its name be removed from financial transactions.²

These deceptive practices included the willing participation by several Western financial institutions, as described below.

3. National Iranian Oil Company

As this Court has found, NIOC “is owned, controlled, and managed by the Government of Iran. A large cash flow of money was funneled to terrorist organizations through the NIOC.” *In re Terrorist Attacks on Sept. 11, 2001*, 2011 WL 13244047, at *8 (emphasis added). NIOC used its oil and natural gas revenues to launder money for the IRGC, often using Bank Markazi for this purpose. NIOC also obtained letters of credit from western banks to provide financing and credit to the IRGC.

The U.S. government designated NIOC as a Specially Designated National pursuant to Executive Order 13382. In September 2012, the Treasury Department reported to Congress that NIOC is an agent or affiliate of the IRGC. Congress found that NIOC “provide[s] significant support to Iran’s Revolutionary Guard Corps and its affiliates.” Iran Threat Reduction and Syria Human Rights Act of 2012, Pub. L. 112-158, § 312, 126 Stat. 1214, 1249 (Aug. 10, 2012).³

B. Iran Requires Access to U.S. Dollars and U.S. Dollar-Clearing Mechanisms

Some 60 percent of Iranian government revenues – and 90 percent of Iran’s export revenues – originate from the sale of oil and gas, a market that is largely denominated in U.S. dollars. These

² “Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism,” *supra*, at fn.1.

³ After the events giving rise to the claims in the underlying action, in 2016 the U.S. government withdrew this determination as part of the now-defunct Iranian nuclear deal.

dollars are held in Eurodollar accounts outside of the U.S. Payment transactions in the Eurodollar market are settled through correspondent accounts in the U.S.⁴ As stated above, the subpoena recipients are banks that Plaintiffs either know or have a reasonable basis to believe processed certain stages of Eurodollar transactions through the U.S. on behalf of Iran, its agents and instrumentalities, and/or their correspondent banks.

Information underlying a transaction is conveyed through several networks, including (1) SWIFT-NET, a private financial messaging network operated by the Society for Worldwide Interbank Telecommunication (“SWIFT-Brussels”); (2) the CHIPS messaging service; and (3) FedWire (Plaintiffs requested messages from all three of these services, along with others, as relevant messages also include, *inter alia*, email and Telex). There are several hundred message types among these networks, although Plaintiffs only require certain specific message times. For instance, SWIFT message type (“MT”) 103 documents the originator, beneficiary, and intermediaries to a transaction. Other messages include “free format” fields where bank employees can communicate with each other about a particular transaction.

To ensure that U.S. financial institutions that process international wire transfers do not assist Iran in supporting international terrorism and weapons proliferation or facilitate other prohibited transactions, U.S. financial institutions have been (and are) required to monitor and screen all electronic funds transfer payment orders by using a combination of sophisticated computer systems, software algorithms tuned to detect suspicious activity, and personnel trained in anti-money laundering/counter-financing of terrorism (“AML/CFT”) law, regulations, policies

⁴ “A correspondent bank account is a domestic bank account held by a foreign bank, similar to a personal checking account used for deposits, payments and transfers of funds. Correspondent accounts facilitate the flow of money worldwide, often for transactions that otherwise have no other connection to New York, or indeed the United States.” *Licci ex rel. Licci v. Lebanese Canadian Bank, SAL*, 732 F.3d 161, 166 n.3 (2d Cir. 2013) (internal citations and quotation marks omitted).

and procedures. These computer systems and personnel monitor and screen, *inter alia*, the data entered in SWIFT payment order message fields. Banks in New York that process most of the world's dollar-denominated payments, trade finance, commodities, derivatives, and foreign exchange transactions use these automated systems and expert personnel to prevent Iran and other sanctioned entities (as well as terrorists, money launderers, and other criminals) from illicitly accessing the U.S. banking system.

However, a number of Western banks, including five of the subpoena recipients (discussed below), have admitted to circumventing these controls on Iran's behalf. They did so through various means, including "stripping"—omitting or replacing the name of Iranian entities from transactional messages—and "covering"—using bank-to-bank payment order messages that do not mention the names of Iranian parties.

C. Defendants Processed U.S. Dollar-Denominated Transactions on Behalf of Iran and Its Agents and Instrumentalities

Each of the subpoena entities played a role in dollar-clearing for Iranian banks. As major American banks, BOA, Citibank, and JPMC provided clearing and settlement of dollar-denominated transactions for thousands of foreign banks through CHIPS and the New York Federal Reserve, presumably pursuant to U.S. Treasury, Federal Reserve Board, and NYSDFS regulatory controls. As noted above, certain other Western banks admitted to circumventing these controls by, *inter alia*, manipulating the content of messaging systems.

Five of the subpoena recipients here have admitted to such conduct.

1. SCB

Subpoena recipient SCB admitted in a Deferred Prosecution Agreement ("DPA"):

Starting in early 2001 and ending in 2007, SCB violated U.S. and New York State laws by illegally sending payments through the U.S. financial system on behalf of entities subject to U.S. economic sanctions. SCB knowingly and willfully engaged in this criminal conduct, which caused both affiliated and unaffiliated U.S. financial

institutions to process transactions that otherwise should have been rejected, blocked, or stopped for investigation pursuant to rules promulgated by [OFAC]⁵ relating to transactions involving sanctioned countries and parties.

Exhibit C (DPA), “Exhibit A – Factual Statement,” ¶ 2. According to the DPA, “[b]etween 2001 and 2006, the CBI sent approximately 2,226 messages with a total value of \$28.9 billion to SCB London. These messages contained the SCBLGB2L code in field 52, and were sent onto SCB New York for processing either as a cover payment of serial bank-to-bank payment.” *Id.* at ¶ 27 (emphasis added). Additionally, “[f]rom 2001 through 2007, in approximately 458 payment messages comprising \$2.3 billion of transactions, SCB London manually inserted its own SWIFT code in field 52” before sending the messages on to SCB New York for processing. *Id.* at ¶ 28 (emphasis added).

Further, during the relevant period, SCB processed thousands of transactions for Iranian banks that are identified as Subject Entities in the *Hake* plaintiffs’ subpoena. “For almost ten years, SCB schemed with the Government of Iran and hid from regulators roughly 60,000 secret transactions, involving at least \$250 billion[.]” Exhibit R (NYSDFS Order Pursuant to Banking Law § 39 dated August 6, 2012), at ¶ 1. Between 2001 and 2007, SCB New York processed *at least* 2,684 payment messages for Bank Markazi/CBI alone. None of these records were produced, even though the relevant period of the subpoena significantly overlaps those years. SCB has admitted to processing transactions responsive to the subpoena, but has failed to produce them.

2. SocGen

Subpoena recipient SocGen admitted that:

Starting in at least 2004, up through and including 2010, SG knowingly and willfully violated U.S. and New York State laws by illegally sending payments

⁵ The Office of Foreign Assets Control (“OFAC”) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against certain foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

through the U.S. financial system in violation of U.S. economic sanctions, which caused both affiliated and unaffiliated U.S. financial institutions to process transactions that otherwise should have been rejected, blocked or stopped for investigation pursuant to regulations promulgated by the Office of Foreign Assets Control of the United States Treasury (“OFAC”) relating to transactions involving sanctioned countries and parties.

EXHIBIT D (DPA), “Exhibit C – Statement of Facts,” at ¶ 4. By SG’s own admission, it “circumvent[ed] U.S. sanctions by omitting or falsifying information on payment instructions sent through financial institutions located in New York County.” *Id.* at ¶ 17. Notably, SG continued its pattern and practice of fraudulent behavior “for a significant Iranian Government Bank until September 12, 2006, one day before the SG’s top management was to meet with the U.S. Department of the Treasury’s Under Secretary for Terrorism and Financial Intelligence regarding Iran’s use of the global financial system.” *Id.* at ¶ 19.

According to the DPA, “SG processed over 9,000 outgoing transactions that failed to disclose an ultimate sanctioned party sender or beneficiary . . . with a total value of more than \$13 billion. The overwhelming majority of these transactions involved an Iranian nexus[.]” *Id.* at ¶ 20. As a consequence of its illicit conduct, SG agreed to pay \$717,200,000 to the U.S. government in forfeiture.

3. BNPP

In a June 2014 Settlement Agreement with OFAC, BNPP admitted to processing thousands of U.S. dollar transactions to or through the United States in apparent violation of the U.S. sanctions regime, which included transactions for Iran. Exhibit E, at ¶ 3-4. In the Statement of Facts annexed to BNPP’s guilty plea to the charge of conspiracy to commit violations of sanctions regulations, BNPP admitted that:

From at least 2004 up through and including 2012, BNPP, the defendant, conspired with banks and other entities located in or controlled by countries subject to U.S. sanctions, including Sudan, Iran and Cuba...to knowingly, intentionally and willfully move at least \$8,833,600,000 through the U.S. financial system on behalf

of Sanctioned Entities in violation of U.S. sanctions laws, including transactions totaling at least \$4.3 billion that involved SDNs.

Exhibit F, at ¶ 14.

Apart from transaction records that BNPP maintains in its routine course of business, the Settlement Agreement indicates that “BNPP cooperated with OFAC by conducting an extensive internal investigation,” which would potentially contain information responsive to the *Hake* plaintiffs’ subpoena. Exhibit E, at ¶ 24. The subpoena requests, *inter alia*, “[r]esponsive portions of any productions or reports prepared either internally or created by a third party that relate to the Subject Entities.” Accordingly, BNPP has two readily-available sources for records: its transaction databases and documents prepared in connection with the aforementioned investigation.

4. HSBC

According to the December 2012 Settlement Agreement entered into between OFAC and HSBC Holdings,⁶ “[i]n January 2001, HBEU approached HBUS with a proposal to clear U.S. dollar transactions for Bank Melli London...through HBEU’s correspondent account with HBUS by utilizing [SWIFT] MT 202 cover payments that would not reference Bank Melli.” Exhibit G, at ¶ 3. The Settlement Agreement also stated:

By July 2001, several HBUS compliance, payments, and business managers, as well as HSBC Group’s Compliance head, were aware that HBEU was discussing with Bank Melli how to structure Iranian-related payments to be processed through HBUS. Although HBUS’ head of Compliance warned HSBC Group’s head of Compliance that OFAC might view HBEU’s formatting instructions to Bank Melli as a willful disregard or evasion of U.S. sanctions, and that the non-transparent nature of the payment messages could make it impossible for either HBEU or HBUS to confirm that any payment would be permissible, neither HSBC Group nor HBEU implemented processes to ensure the Bank Melli payments processed to or through HBUS were authorized or exempt pursuant to U.S. sanctions

⁶ HSBC Holdings is a public limited liability company organized under the laws of the United Kingdom and directly or indirectly owns, *inter alia*, HSBC Bank plc (“HBEU”), a financial institution registered under the laws of England and Wales; and HSBC Bank USA, N.A. (“HBUS”), a national bank chartered under the laws of the United States. HBUS and HSBC are used interchangeably in this Memorandum of Law.

regulations. HBUS proposed that HBEU address these compliance concerns by only processing Bank Melli payments as serial MT 103 messages.

Id., at ¶ 5.

As reflected in the Settlement Agreement, the government's investigation into HSBC's practices revealed that "in October 2003, a senior Group Compliance official found that HBEU was offering U.S. dollar clearing services to six Iranian banks, and that it had 'been manually intervening in the processing of Iranian bank payment instructions...to prevent...the subsequent declaration to OFAC (and possible freezing) of the funds.'" *Id.*, at ¶ 6. Not including transactions covered by authorizations or exemptions:

From on or about March 19, 2004, to on or about June 15, 2010, HSBC Group affiliates processed a combined 203 electronic funds transfers and trade finance transactions in the aggregate amount of \$164,308,904, for the benefit of the Government of Iran and/or persons in Iran, through a financial institution located in the United States in apparent violation of the prohibition against the "exportation ... , directly or indirectly, from the United States ... of any ... services to Iran or the Government of Iran," 31 C.F.R. § 560.204.

Id., at ¶ 21.⁷

According to the Statement of Facts incorporated by reference as part of the DPA with respect to HSBC:

From at least 2000 through 2006, HSBC Group knowingly and willfully engaged in conduct and practices outside the United States that caused HSBC Bank USA and other financial institutions located in the United States to process payments in violation of U.S. sanctions. To hide these transactions, [HSBC] altered and routed payment messages in a manner that ensured that payments involving sanctioned countries and entities cleared without difficulty through HSBC Bank USA and other U.S. financial institutions in New York County and elsewhere.

Exhibit H, at ¶ 63. The total value of OFAC-prohibited transactions on behalf of sanctioned entities in Iran was approximately \$183 million. *Id.* HSBC agreed to forfeit approximately \$1.2 billion to

⁷ Additionally, "on May 24, 2006, the London branch of HBUS acted as a clearing bank in a book entry transfer of 32,000 ounces of gold bullion, valued at \$20,560,000, for the ultimate benefit of Bank Markazi[.]" *Id.*

the U.S. government for its violations. Accordingly, HSBC clearly engaged in transactions on behalf of Bank Melli and Bank Markazi during the relevant period.

5. NatWest

In 2013, RBS admitted that NatWest (and later RBS) processed U.S. dollar transactions to or through the United States in apparent violation of the U.S. sanctions regime, which included transactions for Iran. According to the Settlement Agreement,

In 1997, National Westminster Bank (“NatWest”) - which RBS acquired in March 2000 - began acting as a correspondent bank for Bank Melli Iran (“Bank Melli”) and its wholly-owned UK subsidiary, Melli Bank Plc (“Melli Plc”). As part of its operations in serving as a correspondent bank, RBS processed U.S. Dollar (“USD”) transactions for and on behalf of Bank Melli and Melli Plc and these banks’ customers. NatWest (and later RBS) conducted USD payments for the Iranian banks by sending [SWIFT] MT103 payment messages directly to non-U.S. beneficiary banks, and SWIFT MT202 payment messages (or “cover payments”) to U.S. clearing banks. Although the payment messages sent to non-U.S. beneficiary banks included complete payment information, including the names of the Iranian banks and customers, the payment instructions sent to U.S. financial institutions did not include any references to the Iranian parties.

Exhibit I, at ¶ 3. RBS admitted to processing U.S. dollar payments through the United States – in violations of the sanctions regime that included Iran – until late 2009. *Id.* at ¶ 15.

IV. THE SUBPOENA REQUESTS⁸

A. The *Hake* Subpoena

The *Hake* plaintiffs served the same Fed. R. Civ. P. 45 subpoena on every defendant to this motion. The subpoena seeks certain records relating to a list of “Subject Entities,” which constitute the three *Hake* defendants along with some of their aliases and agents, as identified by the U.S.

⁸ The subpoenas overlap considerably; as a result, information requested under each subpoena is relevant to each of the underlying suits. As a result, where a third party has received subpoena relating to both *Gill* and *Hake*, Plaintiffs have, where possible, negotiated a protective agreement and order permitting the use of documents from each subpoena in each suit, as well as other suits in certain circumstances.

Treasury, and state-controlled Bank Saderat (which allegedly transferred funds to Hezbollah other terror groups on CBI's behalf).

The subpoenas request:

1. Transactional Records involving any Subject Entity, including any Transaction Records relating to any Transaction relating to or involving or including as a party or intermediary any Subject Entity, including as to each, but not limited to:
 - a. Documents sufficient to identify the originators, intermediaries and beneficiaries, including any financial institutions, accounts, or Correspondent Accounts involved in facilitating any step of the Transaction;
 - b. Documents sufficient to identify the name and number of the account of the originators, intermediaries, and beneficiaries of each Transaction; and
 - c. Documents sufficient to identify the date and value (in U.S. Dollars) of any Transaction.
2. Non-privileged documents and communications sufficient to identify and/or summarize all Transactions or analysis relating to or involving the Subject Entities, including:
 - a. Responsive portions of any productions or reports prepared either internally or created by a third party that relate to the Subject Entities; and
 - b. Responsive portions of any reports or analyses whether prepared by You or received by You relating to the Subject Entities.

See, e.g., Exhibit J (Subpoena to HSBC).

B. The *Gill* Subpoenas

Mr. Gill issued two subpoenas seeking certain records relating to lists of "Subject Entities."

The "Subject Entities" in the first subpoena list entities identified as related to Hezbollah and, in the second, to the IRGC. Both sets of subpoenas request:

1. Transactional Records involving any Subject Entity, including any Transaction Records relating to any Transaction to, by, for, for the benefit of, or including as an intermediary any Subject Entity, including as to each, but not limited to:

- a. Documents sufficient to identify the originators, intermediaries and beneficiaries, including any financial institutions, accounts, or Correspondent Accounts involved in facilitating any step of the Transaction;
- b. Documents sufficient to identify the name and number of the account of the originators, intermediaries, and beneficiaries of each Transaction; and
- c. Documents sufficient to identify the date and value (in U.S. Dollars) of any Transaction.

See, e.g., Exhibit K (Subpoena to JPMC).

V. THE SUBPOENA RECIPIENTS' NON-COMPLIANCE

Of the eight subpoena recipients at issue here, six (Citibank, BOA, JPMC, SCB, SocGen, and BNPP) produced spreadsheets providing limited details to small sets of transactions, which are insufficient for Plaintiffs. The other two (HSBC and NatWest) have produced *nothing*, even though both of them entered into agreements with U.S. regulators in which they admitted to performing thousands of transactions on behalf of Iran. All eight subpoena recipients entered into protective orders that have been entered by the courts in the *Hake* and *Gill* actions.

A. Six Subpoena Recipients Have Made Insufficient Productions

JPMC, Citibank, BOA, SCB, SocGen, and BNPP have produced spreadsheets with limited information that require supplementation to comply with the subpoenas at issue. *First*, the spreadsheets are too limited in scope—particularly given (1) the hundreds of billions of dollars Iran moved during the relevant time period through (2) its primary banks (including principally the *Hake* defendants) for (3) some of its largest entities (such as subpoena Subject Entities NIOC, Kala Naft (*Gill* only), and Khatam al-Anbiya (*Gill* only)), and with the (witting or unwitting) assistance of (4) the subpoena recipients, which are some of the largest banks in the world.

Citibank and BOA, despite being two of the largest banks in the world and performing a significant amount of the dollar clearing that occurs in the U.S.,⁹ initially produced spreadsheets listing a total of *four* transactions (BOA later listed another nine), nearly a year and a half after receiving the *Gill* subpoenas and months after receiving the *Hake* subpoena. They each flatly refused to discuss search terms or parameters for months while the parties negotiated a protective order, and then produced spreadsheets based on criteria they unilaterally decided upon. Unlike *any* of the other subpoena recipients, Citibank and BOA also refused to produce executed transactions, producing only transactions that they had blocked pursuant to Treasury and other regulations requiring correspondent banks to block transactions relating to entities designated under certain sanctions regimes (including sanctions for participation in Iran’s terror apparatus).¹⁰ However, as Plaintiffs’ counsel explained to counsel for Citibank and BOA, transactions even with IRGC or Hezbollah-controlled entities may not have been blocked because, *inter alia*, they occurred before those entities were designated, failures in a bank’s compliance systems, or bank misconduct. Plaintiffs have attempted to work productively with both banks, to no avail. *See Exhibit L* (correspondence with counsel for Citibank); *Exhibit M* (correspondence with counsel for BOA).

JPMC, on the other hand, agreed to produce blocked and unblocked transactions, and even agreed to search terms during the negotiation of the protective order. It claimed that the search terms produced excessive nonresponsive “hits,” so Plaintiffs narrowed the terms. Although it is unclear if JPMC implemented the revised terms, it produced two spreadsheets listing transactions,

⁹ Citi claims to be “the largest user of SWIFT.” *See* <https://icg.citi.com/mss/dcc/swift/>. BOA is the second largest bank in the U.S. and a major participant in the CHIPS and SWIFT systems. Neither bank denies having responsive records.

¹⁰ On March 15, 2019, the deadline to file this motion, counsel for Citibank presented a proposal whereby it would produce limited records of transactions, including unblocked transactions—and at Plaintiffs’ expense. However, this does not appear to be a commitment to fully produce responsive documents. Plaintiffs respectfully request that the Court order Citibank to comply with the subpoenas and without shifting costs to Plaintiffs.

and stated that it is still searching for transactions “involving a few other subject entities in the subpoenas” and the two Subject Entities unique to the *Hake* subpoena. See Exhibit N (correspondence with counsel for JPMC). Others, like SCB, produced spreadsheets listing hundreds of transactions, but their admissions in DPAs strongly suggest they should have listed thousands more.

Second, the spreadsheets each of these six subpoena recipients produced are too limited in detail.¹¹ Central to Mr. Gill’s ability to trace Iranian assets around the world and the *Hake* plaintiffs’ ability to identify *flows* from the *Hake* defendants to IRGC and Hezbollah-related entities are several pieces of metadata intrinsic to SWIFT, CHIPS and FedWire transactional messages, including information such as reference numbers that remain consistent and allow a transaction to be tracked from originator to ultimate beneficiary. Even where certain parties have stripped out information identifying Iranian parties, the *metadata* – such as reference numbers – permit Plaintiffs to reconstruct transactional message flows.¹² For instance, Plaintiffs can cross-reference metadata from other data sets, including productions from more compliant subpoena recipients (some banks have produced thousands of transactions with dozens of information fields), to fill in the missing parties to an electronic funds transfer transaction.

For example, the spreadsheets produced by JPMC indicate a 2005 transaction on behalf of Oriental Oil Kish, which was later designated as an IRGC agent.¹³ The spreadsheet indicates that Oriental Oil Kish held an account with SCB, but not which branch or country (the transaction does

¹¹ Further, BNPP only produced its purportedly responsive spreadsheet on March 14, 2019, the day before the deadline to file this motion, and only after repeated prompting from counsel.

¹² One of the subpoena recipients not at issue here produced a SWIFT MT-999 communication relating to an Iranian transaction that instructed, “address y[ou]r pay[men]t instruction directly to them . . . (without mentioning our Hamburg br[anch], or any Iranian entity[.], insert only the ref[erence] number of [letters of guarantee] yours and ours).”

¹³ See Treasury Press Release, *supra* at n1.

not appear in the spreadsheets produced by SCB). Without metadata, Plaintiffs cannot tell if, for instance, any of the *Hake* defendants initiated these transactions since the counterparties are not visible from the data provided.

The metadata contained in a SWIFT message is functionally no different from the user-generated fields. More than one subpoena recipient provided this information, and there is no reason why the defendants here could not also have done so. As shown above, the subpoenas request the transactional *messages* themselves, not spreadsheet summaries with information chosen solely by the subpoena recipients. In fact, at Mr. Gill's request, SCB produced parts of the actual SWIFT messages corresponding to the transactions it identified as responsive to the *Gill* subpoenas (but not the *Hake* subpoena). Indeed, Plaintiffs would accept production of the responsive original SWIFT, CHIPS, FedWire, Telex, and e-mail messages from each subpoena recipient at issue here, in lieu of production of more complete spreadsheets.

Third, only two banks (not at issue here) have produced communications relating to the transactions, which are requested in the *Hake* subpoenas. In addition to the most common SWIFT messages at issue, SWIFT also permits banks to generate free-format communications and these should have been produced pursuant to the *Gill* subpoenas. Given that many of the entities listed in the subpoenas were or became designated, dozens of communications were likely sent between banks discussing these transactions.¹⁴ For example, these communications help show the end-to-end routing path of relevant transactional messages from an originator in Country A to an intermediary bank in Country B, through correspondent banks and CHIPS clearing in New York,

¹⁴ Dozens of HSBC communications relating to these transactions were exhibits to a Senate investigation into HSBC's dealings with Iranian entities. See U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History, Hearing Before the Permanent Subcomm. on Investigations of the Comm. on Homeland Security and Governmental Affairs, 112th Cong., S. Hrg. 112-597 (July 17, 2012), available at <https://www.govinfo.gov/content/pkg/CHRG-112shrg76061/html/CHRG-112shrg76061.htm>.

to an intermediary bank in Country C, and, finally, to a beneficiary in Country D. Moreover, because only SWIFT messages were stripped, analyzing relevant CHIPS, Fedwire, Telex, and e-mail messages will allow plaintiffs to reconstruct transactions in a way that would be impossible without access to these unmodified communications.

Further, the banks that made insufficient productions, by and large, did not agree on search terms or search parameters, let alone even *discuss* search terms with Plaintiffs. Plaintiffs have no way of knowing what searches were conducted or which databases were searched. However, as shown above, when one bank produces information concerning a transaction record that another bank should have but failed to produce, there are self-evident concerns regarding the thoroughness and diligence of the defendants' searches and productions.

As the DPAs show, many banks conducted internal investigations and/or were the subjects of governmental investigations concerning transactions they executed on behalf of Iranian entities. Documents and transactions reviewed, produced or prepared in connection with these DPAs may therefore serve as important sources of relevant records that are responsive to the subpoenas. The DPAs were filed in, and investigation results were transmitted to U.S. authorities in, the Southern and Eastern Districts of New York and the District of Columbia and are presumably in the possession, custody or control of the defendants, which should search them for responsive records.

B. Two Subpoena Recipients Have Not Produced at All

Despite Plaintiffs' best efforts, HSBC and NatWest have not produced any information whatsoever. As discussed above, each admitted to illegally processing billions of U.S. dollar-denominated transactions through the U.S. on behalf of Iran and its agents and instrumentalities.

1. HSBC

On September 19, 2017, Mati Gill served two subpoenas on HSBC. HSBC entered into discussions with Mr. Gill regarding search parameters and the entry of a protective order. Mr. Gill

agreed to limit the scope of HSBC's *initial* searches to blocked and unblocked transactions exceeding \$10,000, reserving the right to request searches for transactions for lower amounts. HSBC agreed to search for records relating to both blocked and unblocked electronic funds given appropriate search terms. Mr. Gill proposed search terms and, following productive negotiations, the parties agreed to a set of search terms for one of the *Gill* subpoenas. On July 18, 2018, HSBC agreed to start searching for transactions, as well as to propose search terms for the second *Gill* subpoena. However, after repeated requests for updates, HSBC has yet to produce a single transaction responsive to the *Gill* subpoenas or propose any additional search terms. See Exhibit Q, at 1. Since September 24, 2018, HSBC has offered no further search terms.

On June 28, 2018, the *Hake* plaintiffs served a subpoena upon HSBC. Exhibit J. Despite having had several months (and two extensions) to search for and produce responsive records, HSBC has not produced a single transaction response to the *Hake* subpoena or discussed *any* search terms. During a March 13, 2019 telephone conference – two days before Plaintiffs' deadline to file this motion – counsel for HSBC represented that HSBC would need another month to produce records responsive to these subpoenas. Accordingly, Plaintiffs have little choice but to file this motion to compel.

2. NatWest

On June 28, 2018, the *Hake* plaintiffs served a subpoena upon NatWest. Exhibit P. Following repeated messages to counsel inquiring about the status of NatWest's search for and production of responsive records, NatWest reported that it would produce on or about March 22, 2019 – after the deadline for this motion. Accordingly, because NatWest has not yet produced any records despite two extensions, Plaintiffs have little choice but to file this motion to compel production.

VI. LEGAL ARGUMENT

Plaintiffs are entitled to discovery regarding any nonprivileged matter that is relevant to any party's claim or defense. The scope of discovery is set forth in Fed. R. Civ. P. 26 (b)(1):

Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.

This language applies to subpoenas served upon non-parties. *See Citizens Union of City of New York v. Atty. Gen. of N.Y.*, 269 F. Supp. 3d 124, 139 (S.D.N.Y. 2017) (“In general, the relevance standard that applies when seeking discovery from a party also applies to non-parties.”).

Relevance is construed broadly to include “any matter that bears on, or that reasonably could lead to other matter that could bear on any issue that is or may be in the case.” *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 351 (1978); *Maresco v. Evans Chemetics, Div. of W.R. Grace & Co.*, 964 F.2d 106, 114 (2d Cir. 1992). *See also Condit v. Dunne*, 225 F.R.D. 100, 105 (S.D.N.Y. 2004) (“Although not unlimited, relevance, for purposes of discovery, is an extremely broad concept.”). Relevant information need not be admissible. Rule 26(b)(1); *Asad Gilani v. Hewlett Packard Co.*, No. 15-CV-05609 (NSR), 2017 WL 4236564 at *1 (S.D.N.Y. Sept. 22, 2017).

The same rule applies to Mr. Gill's post-judgment discovery pursuant to Rule 69. Rule 69 states that, “[i]n aid of the judgment or execution, the judgment creditor . . . may obtain discovery from any person—including the judgment debtor—as provided in these rules [i.e., Fed. R. Civ. P. 26] or by the procedure of the state where the court is located.” Under either Rule 26 or New York law, Mr. Gill may “discover ‘all matter relevant to the satisfaction of [a] judgment,’ permitting ‘investigation [of] any person shown to have any light to shed on the subject of the judgment

debtor's assets or their whereabouts.” *Republic of Argentina v. NML Capital, Ltd.*, 573 U.S. 134, 139 (2014) (citations omitted).

Rule 69 discovery is “quite permissive,” *id.* at 138, and entitles Mr. Gill to “a very broad inquiry regarding the location and identity of” Iran’s assets. *Banco Cent. De Paraguay v. Paraguay Humanitarian Found., Inc.*, No. 01 CIV. 9649 (JFK), 2006 WL 3456521, at *9 (S.D.N.Y. Nov. 30, 2006). *See also id.* (“even if the discovery request is a ‘fishing expedition, . . . this Court recognized long ago that ‘a judgment creditor is entitled to fish for assets of the judgment debtor’”).

A. The Information Sought by Plaintiffs Is Relevant to Their Claims.

The party seeking discovery has the initial burden of showing that the discovery sought is relevant, but “[o]nce relevance has been shown, it is up to the responding party to justify curtailing discovery.” *Fireman’s Fund Ins. Co. v. Great Am. Ins. Co. of N.Y.*, 284 F.R.D. 132, 135 (S.D.N.Y. 2012). The *Hake* plaintiffs seek evidence showing that the *Hake* defendants, as agents and instrumentalities of Iran, participated in funding a terror campaign against U.S. service members, including the *Hake* plaintiffs. Upon reasonable information and belief – including the results of investigations conducted by the U.S. government such as those discussed herein – the financial institutions served with subpoenas all performed U.S. dollar clearing for Iranian entities that include Bank Markazi, Bank Melli and NIOC. Discovery of those financial transactions is therefore relevant to the *Hake* plaintiffs’ claims regarding the financial nexus between the Government of Iran and the terrorist acts it financed and directed. Moreover, the transactions are probative both as to the magnitude and scope of the *Hake* defendants’ direction of millions of U.S. dollars in funds, arms, and materiel to Hezbollah, the IRGC, the IRGC-QF, and their proxies in Iraq, used in carrying out their attacks against Plaintiffs and their family members.

Mr. Gill seeks evidence as to the location of money belonging to Iran, its agents or affiliates. This includes assets seizable in the United States, including assets seizable pursuant to the Terrorism Risk Insurance Act, Pub. L. 107–297, § 201(d)(2)(A), 116 Stat. 2322 (Nov. 26, 2002). But because seizable assets in the U.S. can be difficult to find, Mr. Gill also seeks to uncover flows of Iranian state money to its agents and affiliates linked to terrorism that may be seizable abroad. *See EM Ltd. v. Republic of Argentina*, 695 F.3d 201, 207–08 (2d Cir. 2012) (“It is not uncommon to seek asset discovery from third parties, including banks, that possess information pertaining to the judgment debtor’s assets. . . . Nor is it unusual for the judgment creditor to seek disclosure related to assets held outside the jurisdiction of the court where the discovery request is made.”) *aff’d*, *NML Cap.*, 573 U.S. 134. *See also* Testimony of Patrick L. Clawson, Ph.D., credited in *Flanagan v. Islamic Republic of Iran*, 87 F. Supp. 3d 93, 121 (D.D.C. 2015) (describing successful seizures of Iranian assets abroad in satisfaction of U.S. judgments).

Plaintiffs’ discovery requests therefore meet the elements of Rule 26:

- **The requests are proportional to the needs of the case.** The information sought is central to both the *Hake* case, which is premised on the *Hake* defendants’ transfers of U.S.-dollar denominated assets to Iran’s terrorist agents, and Mr. Gill’s enforcement efforts, which seek to find Iran’s money linkable to its terrorism network.
- **The issues at stake are significant.** The issues involved—Iran’s exploitation of the U.S. financial system to wage a terror campaign against U.S. forces in Iraq and civilians in Israel is clearly significant (and, indeed, the *Hake* court ordered discovery as to them).
- **The amount in controversy is significant.** The amount in controversy—namely, the personal injury and solatium claims of the hundreds of *Hake* plaintiffs (including punitive damages), and Mr. Gill’s \$30 million judgment—is very substantial.
- **Defendants here have vastly greater resources.** The parties’ relative resources favor a ruling compelling disclosure—movants are mostly U.S. service members (some unable to work because of their injuries) and members of their immediate families (many of whom lost their principal breadwinner). Non-movants are some of the largest financial institutions in the world; indeed, several other banks were

able to locate records responsive to the subpoenas without indicating that they incurred any unreasonable costs.

- **The benefit to Plaintiffs outweighs the burden to subpoena recipients.** The requested records relate to central issues in both cases. The subpoena recipients store and search for these records in the ordinary course of their business and locating them should not be unduly burdensome (indeed, other subpoena recipients have or are in the process of preparing productions of records); for instance, to perform “look backs” for clients or government regulators. Moreover, the subpoena recipients that entered into DPAs and consent orders likely assembled responsive records for production to government agencies.
- **The subpoena recipients have relatively greater access to the relevant information,** as is self-evident.

VII. CONCLUSION

For the reasons set forth above, Plaintiffs respectfully request that the Court enter an Order:

1. Compelling each Defendant to produce all records responsive to Plaintiffs’ subpoenas;
2. Compelling Rule 30(b)(6) depositions of a designated representative from each defendant

regarding:

- a. The searches performed and the databases searched regarding the subpoenas at issue;
 - b. All potential sources, databases and custodians of responsive information, including any internal and/or external investigations relating to Iran and/or the Subject Entities in the subpoenas during the relevant period, and where those sources are stored in the U.S. and in what physical and electronic forms;
 - c. A designated representative regarding its databases, record-keeping, system infrastructure with respect to the electronic storage of information, and retention policies and practices; and
3. Granting such other and further relief as justice requires.

Dated: March 18, 2019

Respectfully submitted,

OSEN LLC

By: /s/ Gerard Filitti
Gerard Filitti
Michael J. Radine
William A. Friedman
2 University Plaza, Suite 402
Hackensack, NJ 07601
(201) 265-6400
(201) 265-0303 Fax